

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-154070

(43)Date of publication of application : 08.06.1999

(51)Int.Cl.

G06F 3/12

G06F 13/00

G06F 13/00

(21)Application number : 09-337674

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 21.11.1997

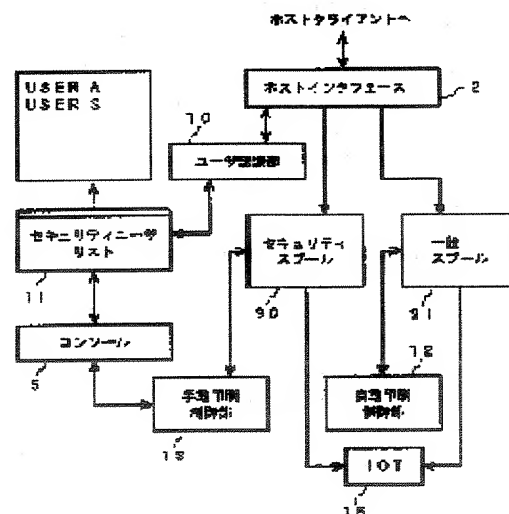
(72)Inventor : ASANO SADAJI

(54) PRINTING CONTROLLER

(57)Abstract:

PROBLEM TO BE SOLVED: To ensure security of printing data transfer, based upon the FTP protocol.

SOLUTION: In a security user list 11, users who are allowed to perform security-printing are registered in advance. A user recognition part 10 stores received data in a security spool 90 on condition that a received user command as an FTP protocol command or information on a path command is registered in the list 11. A manual printing control part 13 reads a stored data out of the security spool 90 and transfers them to a printer engine when a security user name is inputted from a console 5 together with a printing request.



LEGAL STATUS

[Date of request for examination]

19.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-154070

(43) 公開日 平成11年(1999) 6月8日

(51) Int.Cl.⁶

G 0 6 F 3/12
13/00

識別記号

3 5 1
3 5 5

F I

G 0 6 F 3/12
13/00

D

3 5 1 E
3 5 5

審査請求 未請求 請求項の数5 F D (全 6 頁)

(21) 出願番号 特願平9-337674

(22) 出願日 平成9年(1997)11月21日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 浅野 貞二

埼玉県岩槻市府内3丁目7番1号 富士ゼ
ロックス株式会社内

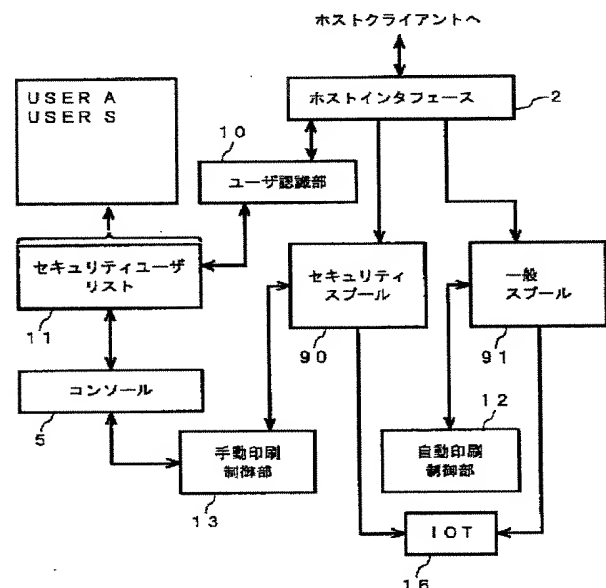
(74) 代理人 弁理士 田中 香樹 (外1名)

(54) 【発明の名称】 印刷制御装置

(57) 【要約】

【課題】 F T P プロトコルを介した印刷データ転送のセキュリティを確保する。

【解決手段】 セキュリティユーザリスト11には守秘印刷を許可されたユーザがあらかじめ登録される。ユーザ認識部10は受信したF T P プロトコルコマンドのユーザコマンドまたはパスコマンド上の情報がリスト11に登録されている場合は、受信データをセキュリティスプール90に格納する。手動印刷制御部13は、コンソール5から印刷要求とともにセキュリティユーザ名が入力された場合に、格納されたデータをセキュリティスプールから読み出してプリンタエンジン1bに転送する。



【特許請求の範囲】

【請求項 1】 F T P プロトコルを介して受信した印刷データを印刷するプリントサーバの印刷制御装置において、

セキュリティユーザ識別情報を登録したリストと、
受信した前記印刷データが守秘印刷ファイルであるか否かを、F T P プロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、
前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、
セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、
前記セキュリティユーザ情報および印刷開始指示の入力にตอบสนองして前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、
前記印刷データを印刷するプリンタエンジンとを具備したことを特徴とする印刷制御装置。

【請求項 2】 前記印刷開始指示手段が、入力されたセキュリティユーザ情報が前記リストに登録されている場合に、前記手動印刷制御手段を有効にする許可信号を出力するように構成されていることを特徴とする請求項 1 記載の印刷制御装置。

【請求項 3】 前記手動印刷制御手段が、前記許可信号を受けた後、さらに前記セキュリティユーザ情報および前記守秘印刷データ格納手段に格納されているユーザ識別情報の一致を条件として前記守秘印刷データ格納手段から印刷データを読み出すように構成されていることを特徴とする請求項 2 記載の印刷制御装置。

【請求項 4】 前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザの名称であって、
前記守秘印刷ファイル認識手段は、前記 F T P プロトコルコマンドのユーザコマンドに含まれるユーザ名が前記リストのユーザ名称に含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 1 記載の印刷制御装置。

【請求項 5】 前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザにセキュリティ用として割り当てられたパスワードであって、
前記守秘印刷ファイル認識手段は、前記 F T P プロトコルコマンドのパスコマンドに含まれるパスワードが前記リストのパスワードに含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 1 記載の印刷制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、印刷制御装置に関し、特に、ネットワークを介して接続された印刷装置（以下、「プリンタ」という）で守秘印刷ファイルを印刷するのに好適な印刷制御装置に関する。

【0002】

【従来の技術】ネットワークにコンピュータを接続したシステム形態として、汎用大型コンピュータつまりメインフレームを中心とした垂直型ネットワークが知られている。また、近年は、コンピュータ・システムのダウンサイジング（小型化）傾向により、ローカル・エリア・ネットワーク（L A N）に複数のワークステーションを接続したシステム形態が増加している。

【0003】このようなネットワーク環境下におかれたプリンタにおいて、機密保持を必要とするファイルつまり守秘印刷ファイルを印刷する場合がある。守秘印刷ファイルを安全に印刷するには、印刷要求者や予め守秘印刷ファイルを出力する資格を与えられているオペレータがプリンタのコンソール上で直接操作をして印刷を実行するのが最も望ましい。

【0004】しかし、そのためには有資格者を、守秘印刷データの転送開始から印刷終了までプリンタに拘束する必要がある、実現が容易ではない。この問題点を解消するため、例えば、特開平 7-134681 号公報では、垂直型ネットワークにおける守秘印刷ファイルの印刷制御装置が開示されている。この印刷制御装置では、印刷データの転送時に該印刷データに付加されるジョブ情報を利用して、有資格者を拘束することなく守秘データの保護ができるようにしている。

【0005】

【発明が解決しようとする課題】上記の印刷制御装置では、次のような問題点がある。水平型ネットワークに接続されるワークステーションやプリンタは、互いに共通する通信プロトコルを通じて会話やデータの授受をしている。

【0006】水平型ネットワークで使用される通信プロトコルの種類は多く、ネットワーク上のワークステーションやプリンタがすべての通信プロトコルに対応することは困難である。そこで、現状のプリンタに最も一般的に実装されていると思われる標準的なファイル転送プロトコルである F T P プロトコルを少なくとも実装することにより、印刷データをファイルとしてプリンタに転送する方式をとることが多い。

【0007】しかし、F T P プロトコルの規約上には守秘印刷ファイルの転送に関する規定はなく、セキュリティ確保の観点からは不十分であった。したがって、標準化されたファイル転送プロトコルである F T P プロトコルを変更することなく印刷ファイルから守秘印刷ファイルを識別してセキュリティを確保することができる方式が要望されていた。

【0008】本発明は、上記問題点を解消し、汎用的なファイル転送プロトコルを変更することなく守秘印刷ファイルを区別することができる印刷制御装置を提供することを目的とする。

【0009】

【課題を解決するための手段】上記の課題を解決し、目的を達成するための本発明は、F T Pプロトコルを介して受信した印刷データを印刷するプリントサーバの印刷制御装置において、セキュリティユーザ識別情報を登録したリストと、受信した前記印刷データが守秘印刷ファイルであるか否かを、F T Pプロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、前記セキュリティユーザ識別情報および印刷開始指示の入力に応答して前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、前記印刷データを印刷するプリンタエンジンとを具備した点に特徴がある。

【0010】上記特徴によれば、F T Pプロトコルコマンド上のユーザ識別情報が、予定のリスト上にあるか否かによって印刷データが守秘印刷ファイルであるか否かが判断され、その判断結果によって守秘印刷ファイルは守秘印刷データ格納手段に格納される。さらに、この守秘印刷ファイルはセキュリティユーザ識別情報が入力したときにプリンタエンジンに読み出される。

【0011】

【発明の実施の形態】以下、本発明の実施形態を図面を参照して詳細に説明する。図2は、本発明の一実施例に係るプリント制御装置を含むプリントサーバの構成を示すブロック図である。同図において、プリントサーバ1はプリンタ制御装置1aとプリンタエンジンつまりイメージ出力端末(I O T) 1bとからなる。プリンタ制御装置1aはホストインタフェース(I / F) 2を通じてクライアントホスト3から印刷データを受信する。受信された印刷データはラスタライズされた後、プリンタインタフェース(I / F) 4を通じてI O T 1bに転送されて印刷される。

【0012】プリンタ制御装置1aはキーボード等の入力手段およびディスプレイ装置を含む操作装置(コンソール) 5と、ROM6、RAM7およびCPU8からなるマイクロコンピュータで実現できる。なお、補助記憶装置として固定ディスク装置9が設けられる。

【0013】プリントサーバ1のホストインタフェース2およびクライアントホスト3はF T Pプロトコルを実行するプログラム、すなわちF T PサーバプログラムおよびF T Pクライアントプログラムをそれぞれ実行する

機能を有している。

【0014】図1は、前記プリントサーバ1の要部制御機能を示すブロック図である。F T Pサーバプログラムを実行するホストインタフェース2はF T Pプロトコル処理を実行してクライアントホスト3から印刷データを受信する。ホストインタフェース2はF T Pのログイン要求時に、受信したF T Pコマンドのユーザコマンド(USER)のパラメータの一つとして記述されているユーザ名が有資格者名であるか否かを判別する。具体的には、守秘印刷ファイルを認識する手段としてのユーザ認識部10において、前記ユーザコマンドとセキュリティユーザリスト11に登録されているセキュリティユーザ情報としてのセキュリティユーザ名すなわち守秘印刷ファイルの印刷を許可されている有資格者名とを比較して識別する。セキュリティユーザ名はあらかじめコンソール5からオペレータによって入力されている。図示の例ではユーザAとユーザSとがセキュリティユーザとして登録されている。

【0015】セキュリティスプール90には、前記ユーザコマンドがセキュリティユーザリスト11上のセキュリティユーザ名に含まれていた場合に、受信した印刷データが格納される。一方、一般スプール91には、前記ユーザコマンドがセキュリティユーザリスト11上のセキュリティユーザ名に含まれていなかった場合に、受信した印刷データが格納される。

【0016】一般スプール91に格納された印刷データは、ひとつのプリントジョブ分の印刷データがそろったときに自動印刷制御部12によって順次I O T 1bに自動的に転送される。また、セキュリティスプール90に格納された印刷データは、手動印刷制御部13によってユーザ名の確認処理を経た後、I O T 1bに転送される。

【0017】コンソール5は、ユーザ名が入力されると、そのユーザ名がセキュリティユーザリスト11に登録されているかどうかを判別し、ユーザ名が登録されている場合に、手動印刷制御部13を有効にする許可信号を出力する。手動印刷制御部13は、コンソール5から前記許可信号を受信すると、その次にコンソール5から入力されるユーザ名を、セキュリティスプール90に印刷データとともに格納されているユーザ名と比較する。比較の結果、両ユーザ名が一致していた場合に、セキュリティスプール90から印刷データを読み出してI O T 1bに転送する。

【0018】上記プリンタ制御装置の処理をフローチャートを参照して説明する。図3においてステップS1では、F T Pコマンドを受信したか否かを判断し、判断が肯定ならばステップS2に進み、ユーザコマンドがセキュリティユーザリスト11に登録されているか否かを判断する。この判断が肯定ならばステップS3に進み、受信した印刷データをセキュリティスプール90に格納す

る。ステップS2が否定ならばステップS4に進み、一般スプール91に受信した印刷データを格納する。

【0019】図4は印刷時のフローチャートである。ステップS10では、印刷要求を待つ。コンソール5から印刷要求が入力されるとステップS11に進む。ステップS11では、ユーザ名の入力を促す表示をコンソール5の表示画面に出力する。ステップS12では、入力されたユーザ名がセキュリティユーザリスト11に登録されているか否かを判断する。この判断が肯定ならばステップS13に進み、セキュリティスプール90に受信した印刷データとともに格納されているユーザ名と、コンソール5から印刷要求とともに入力されたユーザ名とが一致しているか否かを判断する。

【0020】ユーザ名が一致したならばステップS14に進み、セキュリティスプール90上の印刷データをIOT1bに転送する。ユーザ名が一致しない場合、またはユーザ名がセキュリティユーザリスト11に登録されていない場合は、ステップS12、S13からステップS15に移行する。ステップS15では、例えば「印刷不可」の表示をコンソール5に出力するエラー処理をする。

【0021】図5は、クライアントホスト3とプリントサーバ1との間でのFTPプロトコルのコマンドシーケンスである。同図において、クライアントホスト3から接続要求が出されるとプリントサーバ1がこれに回答し、引き続いて、クライアントホスト3からユーザコマンド(USER)とパスコマンド(PASS)が送出され、プリントサーバから、これらのコマンドの回答があるとログイン成功が確認される。ログインが成功した後は、目的に応じて種々のコマンドシーケンスを取り得るが、ここでは、ファイル転送を目的とした簡単なシーケンスを一例としてあげている。

【0022】ログイン成功の後、クライアントホスト3はタイプコマンド(TYPE)により、バイナリやASCIIといったファイルタイプを知らせる。ファイルタイプにより転送方式が異なるからである。さらに、クライアントホスト3は、ポートコマンド(PORT)により、ファイル転送に必要なポート番号をプリントサーバ1に通知する。最後に、クライアントホスト3はストアコマンド(STOR)を発行して、転送するファイル名とファイル転送要求をする。

【0023】ストアコマンドを受けとったプリントサーバ1は先に受けとったポートコマンドのポート番号を用いてデータ転送用の新たなコネクションを開設する。クライアントホスト3はプリントサーバ1からストアコマンドに対する転送許可応答を受信後、プリントサーバ1に対するデータの転送を開始する。データの終了を示すコマンドEOFをプリントサーバ1が受けとった後、プリントサーバ1からの終了確認応答をもってデータ転送は終了する。上述の実施形態では、上記FTPシーケ

スで必ずクライアントホスト3から送出されるユーザコマンドのパラメータの一つとして設定されるユーザ名を判別してセキュリティ処理をした。

【0024】続いて、本願発明の第2実施形態を説明する。この第2実施形態では、図5に示したシーケンスにおけるパスコマンド(PASS)のパラメータとして設定されたパスワードに基づいてセキュリティユーザの判別をする。したがって、前記セキュリティユーザリスト11は図6のように変形する。図6において、セキュリティユーザリスト11ではそれぞれのユーザ名には二つのパスワードが登録されている。第1のパスワード(パス1)は、一般ユーザのパスワードであり、第2のパスワード(パス2)は、セキュリティユーザのパスワードである。すなわち、二つのパスワードをもつことによって、例えばユーザAは、一般ファイルを印刷したいときは、ユーザ名(USERA)とパス1(com)をパスコマンドに記述し、セキュリティファイルを印刷したいときには、ユーザ名(USERA)とパス2(SEC)をパスコマンドに記述するようにする。

【0025】この第2実施形態においては、前記ユーザ認識部10は、ユーザコマンドとパスコマンドとを受信した時点でパスコマンドに記述されているパスワードがセキュリティユーザリスト11に登録されているパス1であれば、受信した印刷データを前記一般スプール91に格納し、パスワードがパス2であれば、受信した印刷データをセキュリティスプール90に格納する。

【0026】また、セキュリティスプール90に格納されている印刷データをIOT1bに出力する場合は、コンソール5から入力されたパスワードと図6のセキュリティユーザリスト11のパスワード(パス2)とを比較した結果により手動印刷制御部13を有効にする。そして、さらに、コンソール5から入力されたパスワードがセキュリティスプール90に印刷データとともに格納されているパスワードと一致した場合に印刷データがセキュリティスプール90からIOT1bに転送される。

【0027】第2実施形態では、第1実施形態に関して説明したユーザ名の判別処理がパスワードの判別処理に置き換えられた点を除き、処理内要は図1～図4に示した例と同様である。このように第2実施形態では二つのパスワードのうちいずれがFTPプロトコルコマンドに含まれているかを判断して一般印刷ファイルか守秘印刷ファイルかを区別した。したがって、ユーザは、いずれのパスワードを使用するかによって、自己の印刷要求対象であるファイルを一般スプールおよびセキュリティスプールのいずれか所望のものに格納することができる。

【0028】

【発明の効果】以上の説明から明らかなように、本発明によれば、印刷データの転送に広く使用されているFTPプロトコルコマンドを変更することなく、かつクライアントホスト側、つまり印刷データ供給側のFTPプロ

10

20

30

40

50

グラムに変更を加えることなく守秘印刷ファイルのセキュリティを確保することができる。すなわち、クライアントホスト側では、プリントサーバ側のセキュリティ機能を意識することなく処理が可能であるため、既存のネットワーク上において容易にセキュリティシステムを実現することができる。

【図面の簡単な説明】

【図1】 本発明の一実施形態に係るプリントサーバの要部制御機能を示すブロック図である。

【図2】 本発明の一実施形態に係るプリントサーバの要部ハード構成を示すブロック図である。

【図3】 印刷データのスプール格納処理のフローチャ

*ートである。

【図4】 印刷印刷処理のフローチャートである。

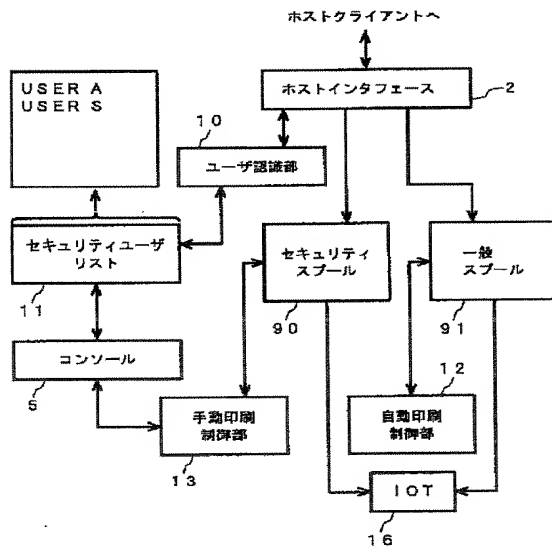
【図5】 F T P プロトコルのシーケンス図である。

【図6】 ユーザ識別情報を登録したリストの一例を示す図である。

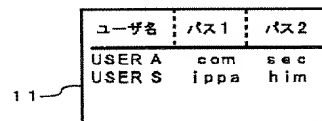
【符号の説明】

1…プリントサーバ、 1a…プリンタ制御装置、 1b…プリンタエンジン、 3…クライアントホスト、 5…コンソール、 10…ユーザ認識部、 11…セキュリティユーザリスト、 13…手動印刷制御部、 90…セキュリティスプール、 91…一般スプール

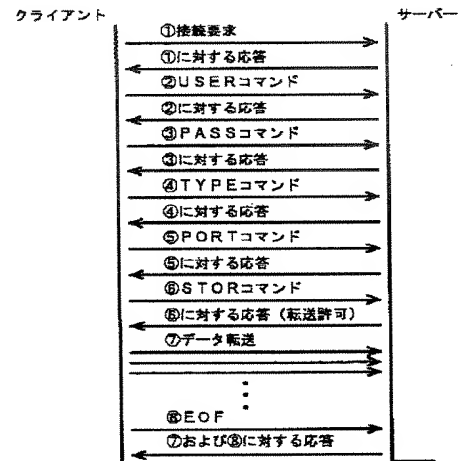
【図1】



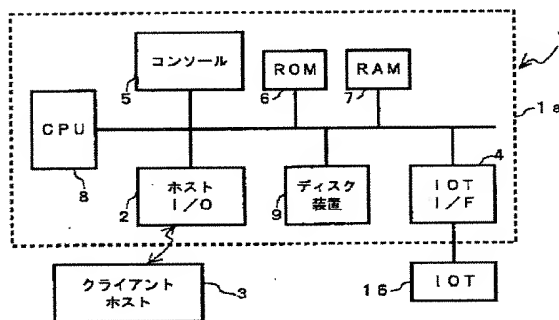
【図6】



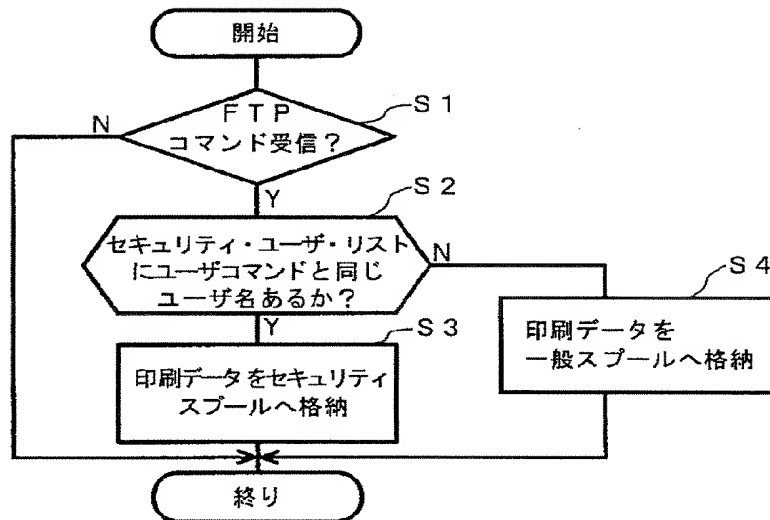
【図5】



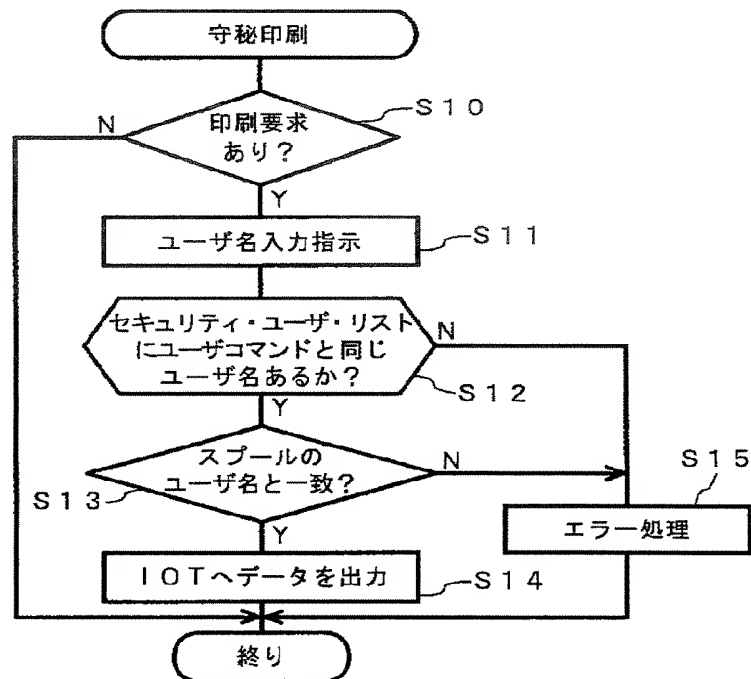
【図2】



【図3】



【図4】



【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成17年7月14日(2005.7.14)

【公開番号】特開平11-154070

【公開日】平成11年6月8日(1999.6.8)

【出願番号】特願平9-337674

【国際特許分類第7版】

G 0 6 F 3/12

G 0 6 F 13/00

【F I】

G 0 6 F 3/12 D

G 0 6 F 13/00 3 5 1 E

G 0 6 F 13/00 3 5 5

【手続補正書】

【提出日】平成16年11月19日(2004.11.19)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】印刷制御装置および印刷制御方法

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

所定のファイル転送プロトコルを介して受信した印刷データを印刷する印刷制御装置において、

セキュリティユーザ識別情報を登録したリストと、

受信した前記印刷データが守秘印刷ファイルであるか否かを、前記ファイル転送プロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、

前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、

セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、

前記セキュリティユーザ情報および印刷開始指示の入力に応答して前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、

前記印刷データを印刷するプリンタエンジンとを具備したことを特徴とする印刷制御装置。

【請求項2】

前記印刷開始指示手段が、入力されたセキュリティユーザ情報が前記リストに登録されている場合に、前記手動印刷制御手段を有効にする許可信号を出力するように構成されていることを特徴とする請求項1記載の印刷制御装置。

【請求項3】

前記手動印刷制御手段が、前記許可信号を受けた後、さらに前記セキュリティユーザ情報および前記守秘印刷データ格納手段に格納されているユーザ識別情報の一致を条件とし

て前記守秘印刷データ格納手段から印刷データを読み出すように構成されていることを特徴とする請求項 2 記載の印刷制御装置。

【請求項 4】

前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザの名称であって、

前記守秘印刷ファイル認識手段は、前記ファイル転送プロトコルコマンドのユーザコマンドに含まれるユーザ名が前記リストのユーザ名称に含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 1 記載の印刷制御装置。

【請求項 5】

前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザにセキュリティ用として割り当てられたパスワードであって、

前記守秘印刷ファイル認識手段は、前記ファイル転送プロトコルコマンドのパスワードに含まれるパスワードが前記リストのパスワードに含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 1 記載の印刷制御装置。

【請求項 6】

所定のファイル転送プロトコルを介して受信した印刷データを印刷する印刷制御方法において、

セキュリティユーザ識別情報を登録したリストを作成し、

受信した前記印刷データが守秘印刷ファイルであるか否かを、前記ファイル転送プロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別し、

前記判別によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を守秘印刷データ格納手段に格納し、

セキュリティユーザ識別情報および印刷開始指示の入力にตอบสนองして前記守秘印刷データ格納手段から印刷データを読み出してプリンタエンジンに該印刷データを供給することを特徴とする印刷制御方法。

【請求項 7】

入力されたセキュリティユーザ情報が前記リストに登録されている場合に、前記守秘印刷データ格納手段から印刷データを読み出してプリンタエンジンに該印刷データを供給することを特徴とする請求項 6 記載の印刷制御方法。

【請求項 8】

前記守秘印刷データ格納手段からの印刷データ読み出しは、前記セキュリティユーザ情報および前記守秘印刷データ格納手段に格納されているユーザ識別情報の一致を条件として行われることを特徴とする請求項 6 記載の印刷制御方法。

【請求項 9】

前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザの名称であって、

前記ファイル転送プロトコルコマンドのユーザコマンドに含まれるユーザ名が前記リストのユーザ名称に含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 6 記載の印刷制御方法。

【請求項 10】

前記リストに登録されているセキュリティユーザ情報は、守秘印刷ファイル転送を許可されたユーザにセキュリティ用として割り当てられたパスワードであって、

前記ファイル転送プロトコルコマンドのパスワードに含まれるパスワードが前記リストのパスワードに含まれている場合に、受信した前記印刷データが守秘印刷ファイルであると判断するように構成されたことを特徴とする請求項 6 記載の印刷制御方法。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】 0001

【補正方法】 変更

【補正の内容】

【0001】

【発明の属する技術分野】

本発明は、印刷制御装置および印刷制御方法に関し、特に、ネットワークを介して接続された印刷装置（以下、「プリンタ」という）で守秘印刷ファイルを印刷するのに好適な印刷制御装置および印刷制御方法に関する。

【手続補正4】

【補正対象書類名】 明細書

【補正対象項目名】 0008

【補正方法】 変更

【補正の内容】

【0008】

本発明は、上記問題点を解消し、汎用的なファイル転送プロトコルを変更することなく守秘印刷ファイルを区別することができる印刷制御装置および印刷制御方法を提供することを目的とする。

【手続補正5】

【補正対象書類名】 明細書

【補正対象項目名】 0009

【補正方法】 変更

【補正の内容】

【0009】

【課題を解決するための手段】

上記の課題を解決し、目的を達成するための本発明は、所定のファイル転送プロトコルを介して受信した印刷データを印刷するプリントサーバの印刷制御装置において、セキュリティユーザ識別情報を登録したリストと、受信した前記印刷データが守秘印刷ファイルであるか否かを、ファイル転送プロトコルコマンド上のユーザ識別情報および前記リストに含まれているセキュリティユーザ識別情報を参照して判別する守秘印刷ファイル認識手段と、前記守秘印刷ファイル認識手段によって守秘印刷ファイルであると判断された印刷データおよび前記ユーザ識別情報を格納する守秘印刷データ格納手段と、セキュリティユーザ識別情報および印刷開始指示を入力する印刷開始指示手段と、前記セキュリティユーザ識別情報および印刷開始指示の入力に応答して前記守秘印刷データ格納手段から印刷データを読み出す手動印刷制御手段と、前記印刷データを印刷するプリンタエンジンとを具備した点に特徴がある。

【手続補正6】

【補正対象書類名】 明細書

【補正対象項目名】 0010

【補正方法】 変更

【補正の内容】

【0010】

上記特徴によれば、所定のファイル転送プロトコルコマンド上のユーザ識別情報が、予定のリスト上にあるか否かによって印刷データが守秘印刷ファイルであるか否かが判断され、その判断結果によって守秘印刷ファイルは守秘印刷データ格納手段に格納される。さらに、この守秘印刷ファイルはセキュリティユーザ識別情報が入力したときにプリンタエンジンに読み出される。